

REMARKS

This Amendment is filed in response to the Final Office Action mailed Feb. 9th, 2005. All objections and rejections are respectfully traversed.

Claims 1-20 and 22-39 are in the case.

Claim 21 has been cancelled.

Claims 14, 19, 20, 22, 27, 28, 30, 35, 36, 38 and 39 were amended to better claim the invention.

No new claims have been added.

Specification

At paragraph 11 of the Office Action, the Specification was objected to as failing to comply with 37 CFR 1.74. The Applicant has amended the Brief Description of the Drawings and page 7, line 27 in accord with the Examiner's comments.

Claim Objections

At paragraph 12 of the Office Action, claims 14, 11, 30, 38, and 39 were objected to as containing informalities. The Applicant has made appropriate corrections.

Double Patenting

At paragraph 13 of the Office Action, claim 21 was objected to under 37 CFR 1.75 as being a substantial duplicate of claim 18. Accordingly, the Applicant has cancelled claim 21.

Claim Rejections – 35 U.S.C. §112

At paragraph 14 of the Office Action, claims 19-20, 27-28 and 35-36 were rejected under 35 U.S.C. §112, second paragraph in relation to several antecedent basis issues. The Applicant has amended the claims to address this rejection.

Claim Rejections – 35 U.S.C. §101

At paragraph 15 of the Office Action, claim 39 was rejected under 35 U.S.C. 101 as directed to non-statutory subject matter. The only explanation given by the Examiner is “[e]lectromagnetic signals may not be patented.”

The Applicant respectfully asserts that the MPEP clearly states that electromagnetic signals may be patented. The Applicant respectfully directs the Examiner’s attention to MPEP 2106 (IV)(B)(1)(c) which states “[h]owever, a signal claim directed to a practical application of electromagnetic energy is statutory regardless of its transitory nature. See *O’Reilly*, 56 U.S. at 114-19; *In re Breslow*, 616 F.2d 516, 519-21, 205 USPQ 221, 225-26 (CCPA 1980).” MPEP 8th edition, Revision 2.

The Applicant seeks to protect electromagnetic signals carrying computer instructions for implementing the novel invention. In an age of widespread digital downloads, an electromagnetic signal claim is particularly relevant. Users commonly download

firmware and drivers from Internet sites that modify or give new capabilities to devices they already own. Such firmware and drivers are embodied in downloadable code that is transferred across a network as electromagnetic signals. One can envision an entity offering a download that configures a user's device to perform the Applicant's novel invention. Accordingly, claim 39 is directed to this type of infringement, making an entity that offers such a download a direct infringer.

Claim Rejections 35 U.S.C. §102

At paragraph 16 of the Office Action claims 8 and 12 were rejected under 35 U.S.C. § 102(b) as being anticipated by Bhanot et al., U. S. Patent No. 5,796,934, issued August 14, 1998 (hereinafter Bhanot).

The present invention, as set forth by representative claim 8, comprises in part:

8. A file server for use in a file server cluster, the file server operatively interconnected with a set of clients using a network protocol, the network protocol being free of support for moving a transport address from a first file server to a second file server, the file server comprising:
 - a cluster interconnect, the cluster interconnect providing a communications link to a partner file server in the file server cluster;
 - a primary data access port for receiving file service operations from file server clients; and
 - a secondary data access port, the secondary data access port only being active when the file server detects that the partner file server has suffered an error condition,*** wherein the file server processes file service operations received via the secondary data access port to provide file service operations to clients of the partner file server.

Bhanot discloses a backup system with a log of transactions. A plurality of clients (Fig. 3, items 301-304) are connected to servers (Fig. 3, items 306, 307), each client

connected to a designate “primary” server by a primary connection. *See* col. 5, lines 5-12. If a server fails, clients establish, via a client interface layer (Fig. 4, item 404), a “secondary” connection (Fig. 3, items 308, 309) to a backup server. *See* col. 6, lines 1-2. Such connection (Fig 4, item 411) is made between the physical network layers (Fig 4, items 405, 410) of the clients and the backup server. *See* col. 6, lines 32-37.

Applicant respectfully urges that Bhanot makes no disclosure of Applicant’s claimed “*a secondary data access port, the secondary data access port only being active when the file server detects that the partner file server has suffered an error condition.*”

While the Applicant teaches a novel *secondary data access port*, Bhanot is completely silent concerning such a feature. As the Examiner points out, Bhanot does disclose forming secondary connections upon failure, but the disclosure does not include of data access ports. Rather than use data access ports, Bhanot simply establishes a traditional low level network connection between a client’s physical network layer and the servers physical network layer. Such connection necessitates the client has prior knowledge of the backup server’s network address or other parameters. Applicant novelly provides greater flexibility by employing the novel *secondary data access port* on the file server.

Accordingly, the Applicant respectfully urges that Bhanot is legally precluded from anticipating Applicant’s claimed invention because of the absence of “*a secondary data access port, the secondary data access port only being active when the file server detects that the partner file server has suffered an error condition.*”

At paragraph 17 of the Office Action claims 1-4, and 11 were rejected under 35 U.S.C. § 102(e) as being anticipated by Sundaresan et al., U. S. Patent Application Publication No. US 2003/0033412 A1, published February 13, 2003 (hereinafter Sundaresan).

The present invention, as set forth by representative claim 1, comprises in part:

1. A method for a first file server to provide file service operations normally performed by a second file server after the second file server suffers an error condition, the first and second file servers operatively interconnected with a set of clients using a network protocol, the network protocol being free of support for moving a transport address from the second file server to the first file server, the method comprising the steps of:

detecting, by the first file server, that the second file server has suffered an error condition;

asserting ownership, by the first file server, of a set of storage devices normally owned by the second file server;

activating, on the first file server, a secondary data access port for receiving connections over a network; and

processing, by the first file server, file service operations directed to the secondary data access port from a set of failover clients, the failover clients accessing the first file server by ***computing a network address associated with the first file server from a symbolic name generated from the second file server***, whereby failover operation is achieved by the client.

Sundaresan discloses a failover technique where a plurality of file servers are divided into clusters. To connect to a server, a client must know both the name of the cluster in which the server resides and the name of the server itself. See paragraph 26, lines 1-11. When a server fails, a client must determine both the cluster and the name of the appropriate backup (second) server. To do this the client must first send a Service Resolution Protocol (SRP) request for server info (Fig. 3, box 303), receive back an SRP reply with the server info (Fig. 3, box 305), and cache the server info into its local cache (Fig 3,

box 309). *See* paragraph 36, lines 1-11. After all of this is complete, the client may then connect to the backup server.

While the Applicant teaches a novel technique for “*computing a network address associated with the first file server from a symbolic name generated from the second file server*,” Sundaresan, in sharp contrast, discloses a lengthy exchange of messages using a Service Resolution Protocol to determine the name and network address for a backup server. Such an exchange of messages introduces unwanted delay and complexity, and exemplifies the type of inefficiency the Applicant’s invention overcomes. The Applicant novelly teaches each client generating a symbolic name for the failover server, based on the name of the primary server. Then using network resolution protocols, a client can resolve symbolic name into a network address. Sundaresan has absolutely no disclosure of such a mechanism.

Applicant respectfully urges that Sundaresan is legally precluded from anticipating Applicant’s claimed novel invention under 35 U.S.C. § 102 because of the absence from Sundaresan of Applicant’s claimed novel “*computing a network address associated with the first file server from a symbolic name generated from the second file server*”

Claim Rejections – 35 U.S.C. §103

At paragraph 18 of the Office Action, claims 5, 7, and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sundaresan in view of Gronke, U. S. Patent

Application Publication No. 2002/0071386, published June 13, 2002 (hereinafter Gronke).

The present invention, as set forth by representative claim 5, comprises in part:

5. A method for a client to continue to access file service operations after a first file server has suffered an error condition, the method comprising the steps of:
 - computing a failover name;*
 - resolving the failover name to a network address; and
 - connecting to a failover file server using the network address and a predetermined alternate data access port.*

Gronke discloses a failover system in which clients communicate to servers using virtual ports. In the event of a failure of a virtual port, a client and server switches to the next functional virtual port and re-establish the connection. *See* paragraph 41, lines 1-5. For example, if communication through port P_n fails, the client and server may switch to port P_1 . *See* paragraph 41, lines 5-10.

The Applicant respectfully urges that the combination of Sundaresan and Gronke does not show Applicant's claimed novel invention relating to "*computing a failover name*" and "*connecting to a failover file server using the network address and a predetermined alternate data access port.*"

While the Applicant novelly teaches a client *computing a failover name* for a failover server to establish a backup connection, both Sundaresan and Gronke are silent concerning such a feature. Sundaresan, in sharp contrast, discloses a lengthy exchange of messages using a Service Resolution Protocol to determine the name and network address of a failover server. Gronke, again dissimilarly, discloses a list of virtual ports, and in the

case of failure of one virtual port, trying another virtual port on the list. Rather than compute any type of failover name, Gronke merely moves down a list of virtual ports until a connection is reestablished.

Further, while Applicant teaches *connecting to a failover file server using the network address and a predetermined alternate data access port*, Sundaresan and Gronke are again silent. Sundaresan's "second server" has a single port (the second port number) through which it handles both its primary and backup roles. See paragraph 36, lines 1-4. Gronke discloses a number of alternate virtual ports, but no single port appears to be a "predetermined alternate." Gronke merely describes selecting one of the many other virtual ports on a list as a substitute.

Accordingly, the Applicant respectfully urges that both Sundaresan and Gronke, taken either singly, or in combination, are legally precluded from rendering Applicant's claimed invention obvious under 35 U.S.C. § 103 because of the absence from both of Applicant's claimed novel "*computing a failover name*" and "*connecting to a failover file server using the network address and a predetermined alternate data access port.*"

At paragraph 19 of the Office Action, claims 9 and 10 were rejected under 35 U.S.C. § 103 as being unpatentable over Bhanot as applied to claim 8, in view of Sundaresan.

The Applicant respectfully notes that claims 9 and 10 are both dependent from independent claims, and the independent claims are believed to be in condition for allowance. Accordingly, the dependent claims are believed to be in condition for allowance.

At paragraph 20 of the Office Action, Claims 14-15, 17-23, 25-31, and 33-39 were rejected under 35 U.S.C. §103(a) as being unpatentable over French et al., U.S. Patent No. 6,745,241, issued on June 1, 2004 (hereinafter French), in view of Sundaresan and Gronke.

The present invention, as set forth by representative claim 14, comprises in part:

14. A method for operating a computer failover system, comprising:
 executing a client computer program on a client computer, the client computer program communicating with a first file server;
 computing, by a file system process communicating with the client computer program, a failover name;
 resolving the failover name to a network address;
 detecting an error condition; and
 connecting, in response to detecting the error condition, to a failover file server port having the network address.

French discloses a method for server failover. Servers are assigned primary and secondary server names (network names) and store this information in local data structures. See col. 8, lines 15-22. If a primary server fails, a secondary server may be reconfigured, either manually or by failover software, to assume the primary server's name and execute the primary server's functionality. See col. 14, lines 56 to col. 15, line 15.

The Applicant respectfully urges that the combination of French, Sundaresan and Gronke does not show Applicant's claimed novel invention relating to "*computing, by a file system process communicating with the client computer program, a failover name.*"

As previously described, the Applicant novelly teaches a client *computing a failover name* for a failover server to establish a backup connection. All three references

are silent concerning such a feature. French, in sharp contrast discloses reassigning an existing primary server's name to the secondary server. Such dynamic reassignment of names may not be possible in many network configurations, and requires undesirable re-configuration. Sundaresan, in sharp contrast, discloses a lengthy exchange of messages using a Service Resolution Protocol to determine a failover name. Finally, Gronke, in sharp contrast, discloses a list of many virtual ports and selecting one of the many possible alternate virtual port in the case of failure.

Accordingly, Applicant respectfully urges that French, Sundaresan, and Gronke, taken either singly, or in combination, are legally precluded from rendering Applicant's claimed invention obvious under 35 U.S.C. § 103 because of the absence from both of Applicant's claimed novel "*computing, by a file system process communicating with the client computer program, a failover name.*"

In the event that the Examiner deems personal contact desirable in disposition of this case, the Examiner is encouraged to call the undersigned attorney at (617) 951-3078.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims.


Applicant respectfully solicits favorable action.

PATENTS
112056-0035
P01-1311

Please charge any additional fee occasioned by this paper to our Deposit Account
No. 03-1237.

Please charge any additional fee occasioned by this paper to our Deposit Account
No. 03-1237.

Respectfully submitted,



James A. Blanchette
Reg. No. 51,477
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500